CLAIMS

What is claimed is:

1. A system for facilitating processing and disposition of a transaction within an access controlled environment, comprising:

an access control facility accessible via a global data processing network and configured to maintain user information, and to permit or deny a user to enter an access controlled environment within a data processing environment and to perform user operations within said access controlled environment;

a transaction management facility operable within said access controlled environment, coupled to said access control facility, and configured to store and maintain transaction data based on said transaction, said user operations, and a security scheme;

an authentication facility operable within said access controlled environment and configured to authenticate said transaction data based on an authentication scheme corresponding to said transaction; and

a billing facility configured to consolidate data related to internal operations performed by said access control facility, said transaction management facility, and said authentication facility to generate and process billing data and to send a billing notice to a responsible party via said global data processing network.

2. The system according to claim 1, wherein said global data processing network is the Internet.

3. The system according to claim 1, wherein said access control facility includes a user registration facility permitting a user to be registered based on predetermined registration

criteria prior to permitting said user to access said access controlled environment.

4. The system according to claim 1, wherein said access control facility permits or denies access based on a user identifier and a user password.

5. The system according to claim 1, wherein said access control facility is further configured to notify said responsible party when a user is denied access to said access controlled environment.

6. The system according to claim 1, wherein said transaction management facility is configured to store and maintain said transaction data based on the type of said transaction.

7. The system according to claim 1, wherein said transaction management facility is further configured to generate internal tracking data corresponding to said user operations within said access controlled environment.

8. The system according to claim 1, wherein said transaction management facility further comprises at least one analysis tool configured to be used by said user to analyze said transaction data within said access controlled environment to facilitate disposition of said transaction.

9. The system according to claim 1, wherein said transaction management facility stores said transaction data in a plurality of formats corresponding to transaction party systems maintained by outside of said access controlled environment.

10. The system according to claim 1, wherein said security scheme corresponds to a predetermined data encryption scheme.

11. The system according to claim 1, wherein said security scheme is set by said user.

12. The system according to claim 1, wherein said security scheme is set automatically based on the type of said transaction.

13. The system according to claim 14, wherein said authentication scheme corresponds to rules of evidence.

14. The system according to claim 1, wherein said authentication scheme is established by said user.

15. The system according to claim 1, wherein said authentication scheme is automatically set by said authentication system based on the type of said transaction.

16. The system according to claim 1, wherein said authentication facility further authenticates said transaction data based said user's identity.

17. The system according to claim 1, wherein said authentication facility further authenticates said transaction data based biometric data related to said user.

18. The system according to claim 1, wherein said authentication facility further authenticates said transaction data based forensic data related to said transaction.

19. The system according to claim 1, wherein said authentication facility further authenticates said transaction data base on forensic data related to said user.

20. The system according to claim 1, wherein said authentication facility authenticates said transaction data prior to said transaction management facility storing and maintaining said data.

21. The system according to claim 1, wherein said authentication facility authenticates said transaction data after said transaction management facility stores and maintains said data.

22. The system according to claim 1, wherein said authentication facility requires said user to enter authentication data related to said transaction data and authenticates said transaction data based upon said authentication data.

23. The system according to claim 1, wherein said billing facility generates a billing record related to said user operations within said access controlled environment.

24. The system according to claim 1, wherein said transaction management facility is further configured to automatically notify said user based upon a change to said transaction data.

25. The system according to claim 24, wherein said transaction management facility notifies said user via an automatically generated electronic mail message.

26. The system according to claim 25, wherein said automatically generated electronic mail message contains a reference to said transaction based on a predetermined level of vagueness.

27. A system for facilitating transaction processing and disposition within an access controlled environment, comprising:

an access control facility accessible via a global data processing network and configured to maintain user information and to permit or deny users to login into an access controlled environment maintained within a data processing environment, said user information including a profile relating to each user of said users, each said profile including a user-specific level of security;

a transaction management facility operable within said access controlled environment, coupled to said access control facility, and configured to store and maintain data related to a transaction involving at least one of said users based on a predetermined security level to facilitate disposition of said transaction within said access controlled environment, and to determine accessibility related to said data for said each user based on said each user's profile;

an authentication facility operable within said access controlled environment and configured to authenticate said data related to said transaction based on a predetermined authentication level set to correspond to said transaction;

a connectivity and communications facility coupled to said access control facility, said transaction management facility, and said authentication facility, said connectivity and communications facility configured to communicate with said access control facility, said transaction management facility, said authentication facility, and external transaction party systems to facilitate disposition of

said transaction based on said data stored and maintained by said transaction management facility; and

a billing facility configured to consolidate data related to internal operations performed by said access control facility, said transaction management facility, and said authentication facility to generate and process billing data and to send a billing notice to a responsible party via said global data processing network.

28. The system according to claim 27, wherein said global data processing network is the Internet.

29. The system according to claim 27, wherein said access control facility includes a user registration facility permitting said each user to be registered based on predetermined registration criteria prior to permitting said each user to access said access controlled environment.

30. The system according to claim 27, wherein said access control facility permits or denies access based on a user identifier and a user password.

31. The system according to claim 27, wherein said access control facility is further configured to notify said responsible party when a user is denied access to said access controlled environment.

32. The system according to claim 27, wherein said access control facility is further configured to permit or deny access to said each user based upon an event related to said transaction.

33. The system according to claim 27, wherein said transaction management facility is configured to store and maintain said data based on transaction type.

34. The system according to claim 27, wherein said transaction management facility is further configured to generate internal tracking data corresponding to an operation performed by at least on of said users within said access controlled environment.

35. The system according to claim 27, wherein said transaction management facility further comprises at least one analysis tool configured to be used by said users to analyze said data within said access controlled environment to facilitate disposition of said transaction.

36. The system according to claim 27, wherein said transaction management facility stores said data in a plurality of formats corresponding to external transaction party systems.

37. The system according to claim 27, wherein said predetermined security level corresponds to a predetermined data encryption scheme.

38. The system according to claim 27, wherein said predetermined security level is set by at least one of said users.

39. The system according to claim 27, wherein said predetermined security level is set automatically based on the type of said transaction.

40. The system according to claim 27, wherein said predetermined authentication level corresponds to rules of evidence.

41. The system according to claim 27, wherein said authentication facility said predetermined authentication level is established by at least on of said users.

42. The system according to claim 27, wherein said predetermined authentication level being automatically set by said authentication system based on the type of said transaction.

43. The system according to claim 27, wherein said authentication facility further authenticates said data based on an identity of at least one of said users.

44. The system according to claim 27, wherein said authentication facility further authenticates said data based on biometric data relating to at least one of said users.

45. The system according to claim 27, wherein said authentication facility authenticates said data prior to said transaction management facility storing and maintaining said data.

46. The system according to claim 27, wherein said authentication facility authenticates said data after said transaction management facility stores and maintains said data.

47. The system according to claim 27, wherein said billing facility generates a billing record related to each operation performed by said users within said access controlled environment.

48. The system according to claim 27, wherein said transaction management facility is further configured to automatically

notify at least one of said users when a change has occurred to said data.

49. The system according to claim 48, wherein said transaction management facility notifies said user via an automatically generated electronic mail message.

50. The system according to claim 49, wherein said automatically generated electronic mail message contains a reference to said transaction based on a predetermined level of vagueness.

51. A system for facilitating transaction processing and disposition within an access controlled environment, comprising:

a plurality of user systems, each user system generating and processing data related to a transaction involving a plurality of parties; and

a controlled access environment operating within a secure data processing system, said secure data processing system coupled to said plurality of user system via a global data processing network, said controlled access environment including a data store for storing and maintaining said data related to said transaction involving said multiple parties, an access control facility for permitting and denying said plurality of user systems to access said access controlled environment during the course of said transaction, an authentication system for authenticating said data within said data store, and a communications facility for notifying said user systems based on said data and for permitting said data processing system to securely interact with externally coupled systems to facilitate disposition of said transaction involving.

52. The system according to claim 51, wherein said global data processing network is the Internet.

53. The system according to claim 51, wherein said access control facility includes a user registration facility permitting said plurality of user systems to be registered based on predetermined registration criteria prior to permitting said plurality of user systems to access said access controlled environment.

54. The system according to claim 51, wherein said access control facility permits or denies access based on a user identifier and a user password.

55. The system according to claim 51, wherein said data store is configured to store and maintain said data in ways corresponding to the type of said transaction.

56. The system according to claim 51, wherein said data store stores and maintains said data based on a predetermined security level corresponding to a predetermined data encryption scheme.

57. The system according to claim 56, wherein said predetermined security level is set based on user preferences corresponding to said user systems.

58. The system according to claim 56, wherein said predetermined security level is set based on user preferences corresponding to said plurality of parties.

59. The system according to claim 51, wherein said predetermined security level is set automatically based on the type of said transaction.

60. The system according to claim 51, wherein said authentication system authenticates said data based on predetermined rules.

61. The system according to claim 60, wherein said predetermined rules are rules of evidence.

62. The system according to claim 51, wherein said authentication system authenticates said data based on a predetermined authentication scheme established based on user preferences.

63. The system according to claim 51, wherein said authentication system authenticates said data based on a predetermined authentication scheme automatically set by said authentication system based on the type of said transaction.

64. The system according to claim 51, wherein said authentication system authenticates said data based on the identity of at least one user corresponding to at least one user system.

65. The system according to claim 51, wherein said authentication system authenticates said data prior to said transaction management facility storing and maintaining said data.

66. The system according to claim 51, wherein said authentication facility authenticates said data after said transaction management facility stores and maintains said data.

67. The system according to claim 51, wherein said transaction management facility is further configured to automatically notify at least one said user system when said data is accessed, said notification being made via said communications facility.

68. The system according to claim 67, wherein said notification is an automatically generated electronic mail message (email).

69. The system according to claim 68, wherein said automatically generated electronic mail message contains a reference to said transaction based on a predetermined level of vagueness.

70. A method for facilitating transaction processing and disposition within an access controlled environment, comprising the steps of:

at an access control facility accessible via a global data processing network, maintaining user information and permitting or denying a user to login into an access controlled environment maintained within a data processing environment;

at a transaction management facility coupled to said access control facility, storing and maintaining data related to a transaction based on a predetermined security level to facilitate disposition of said transaction within said access controlled environment;

at an authentication facility, authenticating said data related to said transaction based on a predetermined authentication level;

at a billing facility, consolidating data related to internal operations performed by said access control facility, said

transaction management facility, and said authentication facility; and

at said billing facility, generating and processing said billing data and sending a billing notice to a responsible party via said global data processing network.

70. The method according to claim 70, wherein said global data processing network is the Internet.

71. The method according to claim 70, wherein said at said access control facility step further comprises the step of: at a user registration facility of said access control facility, permitting a user to be registered based on predetermined registration criteria prior to permitting said user to access said access controlled environment.

72. The method according to claim 70, wherein said access control facility permits or denies access based on a user identifier and a user password.

73. The method according to claim 70, wherein said at said access control facility step further comprises the step of: notifying said responsible party when a user is denied access to said access controlled environment.

74. The method according to claim 70, wherein said transaction management facility stores and maintains said data based on the type of said transaction.

75. The method according to claim 70, wherein said at a transaction management facility step further comprises the step of: generating internal tracking data corresponding to

access and use of said data by users within said access controlled environment.

76. The method according to claim 70, wherein said at a transaction management facility step further comprises the step of: at least one analysis tool of said transaction management facility, analyzing said data within said access controlled environment to facilitate disposition of said transaction.

77. The method according to claim 70, wherein said transaction management facility of said storing and maintaining data step stores said data in a plurality of formats corresponding to associated systems maintained by external systems.

78. The method according to claim 70, wherein said predetermined security level corresponds to a predetermined data encryption scheme.

79. The method according to claim 70, wherein said predetermined security level is set by said user.

80. The method according to claim 70, wherein said predetermined security level being set automatically based on the type of said transaction.

81. The method according to claim 70, wherein said authentication facility authenticates said data based on predetermined rules.

82. The method according to claim 81, wherein said predetermined rules are rules of evidence.

83. The method according to claim 70, wherein said authentication facility authenticates said data based on a predetermined authentication scheme established by said user.

84. The method according to claim 70, wherein said at an authentication facility step further comprises the step of: automatically setting an authentication scheme based on the type of said transaction prior to authenticating said data, and authenticating said data based on said authentication scheme.

85. The method according to claim 70, wherein said authentication facility authenticates said data based on the identity of said user.

86. The method according to claim 70, wherein said authentication facility authenticates said data prior to said transaction management facility storing and maintaining said data.

87. The method according to claim 70, wherein said authentication facility authenticates said data after said transaction management facility stores and maintains said data.

88. The method according to claim 70, wherein said billing data is generated and processed relating to each operation performed by said user within said access controlled environment.

89. The method according to claim 70, wherein said at a transaction management facility step further comprises the

step of: automatically notifying said user when a change has occurred to said data.

90. The method according to claim 89, wherein said user is automatically notified via an automatically generated electronic mail message.

91. The method according to claim 90, wherein said automatically generated electronic mail message contains a reference to said transaction based on a predetermined level of vagueness.

92. A method for facilitating transaction processing and disposition within an access controlled environment, comprising the steps of:

at a user system operated by a user, accessing an access control facility via a global data processing network, said access control facility configured to maintain user information related to said user;

permitting or denying said user system operable access to an access controlled environment maintained within a data processing environment based on a profile related to said user including a user-specific level of security;

at a transaction management facility coupled to said access control facility and operating within said access controlled environment, storing and maintaining data related to a transaction involving said user based on a predetermined security level to facilitate disposition of said transaction within said access controlled environment, said transaction management facility determining accessibility related to said data for said user based on said user's profile;

at an authentication facility operating within said access control environment, authenticating said data related to said transaction based on a predetermined authentication level set to correspond to said transaction;

at a communications facility coupled to said access control facility, said transaction management facility, said authentication facility, and operating within said access controlled environment, communicating with external systems to facilitate disposition of said transaction based on said data stored and maintained by said transaction management facility; and

at a billing facility operating within said access controlled environment, consolidating data related to internal operations performed by said access control facility, said transaction management facility, and said authentication facility, generating and processing billing data, and sending a billing notice based on said billing data to a responsible party via said global data processing network.

91. The method according to claim 90, wherein said global data processing network is the Internet.

92. The method according to claim 90, wherein said access control facility includes a user registration facility permitting a user to be registered based on predetermined registration criteria prior to permitting said user to access said access controlled environment.

93. The method according to claim 90, wherein said access control facility permits or denies access to said access controlled environment based on a user identifier and a user password.

94. The method according to claim 90, further comprising the step of: at said access control facility, notifying said responsible party when a user is denied access to said access controlled environment.

95. The method according to claim 90, wherein said transaction management facility is configured to store and maintain said data in ways corresponding to the type of said transaction.

96. The method according to claim 90, further comprising the step of: at said transaction management facility, generating internal tracking data corresponding to access and use of said data by users within said access controlled environment.

97. The method according to claim 90, further comprising the step of: at least one analysis tool of said transaction management facility, analyzing said data within said access controlled environment and providing a result of said analysis to said user to facilitate disposition of said transaction.

98. The method according to claim 90, wherein said transaction management facility stores said data in a plurality of formats corresponding to associated systems maintained by external systems.

99. The method according to claim 90, wherein said predetermined security level corresponds to a predetermined data encryption scheme.

100. The method according to claim 90, further comprising the step of setting said predetermined security level by said user.

101. The method according to claim 90, further comprising the step of: at said transaction management facility, setting said predetermined security level automatically based on the type of said transaction.

102. The method according to claim 90, wherein said authentication facility authenticates said data based on predetermined rules.

103. The method according to claim 102, wherein said predetermined rules are rules of evidence.

104. The method according to claim 90, wherein said authentication facility authenticates said data based on a predetermined authentication scheme established by said user.

105. The method according to claim 90, wherein said authentication facility authenticates said data based on a predetermined authentication scheme automatically set by said authentication system based on the type of said transaction.

106. The method according to claim 90, wherein said authentication facility authenticates said data based on the identity of said user.

107. The method according to claim 90, wherein said authentication facility authenticates said data prior to said

transaction management facility storing and maintaining said data.

108. The method according to claim 90, wherein said authentication facility authenticates said data after said transaction management facility stores and maintains said data.

109. The method according to claim 90, further comprises the step of: at said billing facility, generating a billing record related to each operation performed by said user within said access controlled environment.

110. The method according to claim 90, further comprising the step of: at said transaction management facility, automatically notifying said user when a change has occurred to said data.

111. The method according to claim 110, wherein said transaction management facility notifies said user via an automatically generated electronic mail message.

112. The method according to claim 111, wherein said automatically generated electronic mail message contains a reference to said transaction based on a predetermined level of vagueness.

113. The system for facilitating processing and disposition of a transaction within an access controlled environment, comprising:

a user system configured to access an access control facility accessible via a global data processing network to download a user interface related to a transaction, said access controlled environment configured to maintain user information, and to permit or deny a user to enter an access controlled

environment within a data processing environment and to perform user operations within said access controlled environment;

a transaction management facility operable within said access controlled environment, coupled to said access control facility, and configured allow said user system to store and maintain transaction data via said user interface based on said transaction and a security scheme, said transaction data including data related to a dispute involving a first party and settlement data related to said dispute;

an authentication facility operable within said access controlled environment and configured to require said user system to enter authentication data related to said transaction data entered via said user interface, said authentication data being based on an authentication scheme corresponding to said transaction;

a billing facility configured to consolidate data related to internal operations performed by said access control facility, said transaction management facility, and said authentication facility to generate and process billing data and to send a billing notice to a responsible party; and

a communications facility coupled to said global data processing network, said transaction management facility, said authentication facility, said access control facility and said billing facility, operable within said access controlled environment, and configured to provide secure communications between external systems and said transaction management facility, said authentication facility, said access control facility and said billing facility, to accept settlement offers from a second party related to said dispute, to provide said settlement offers to said first party, and to allow said first party to accept at least on of said settle offers in order to resolve said dispute.

114. The system according to claim 113, wherein said transaction facility is further configured to request data from said first and second parties based on the type and a status of said transaction, to allow said first party and said second party to update said transaction data based on said request, said authentication facility is further configured to authenticate said updated transaction data, and said communications facility is further configured to provide said transaction data to a decision maker to resolve said dispute.

115. The system according to claim 113, wherein said authentication facility is further configured to authenticate said updated transaction data based on a level of anonymity of said user.

116. A method for facilitating processing and disposition of a dispute involving a plurality of transaction parties within an access controlled environment, comprising the steps of:

at an access control facility accessible via a global data processing network, creating and maintaining user security profiles related to said plurality of transaction parties;

at said access control facility, permitting or denying a user to login into an access controlled environment maintained within a data processing environment based upon said user and at least one of said user security profiles corresponding to said user;

if said user is permitted to login, at said access control facility, providing operative access to said user to a transaction management facility operating within said access controlled environment and configured to store and maintain data related to disputes;

at said transaction management facility, permitting user to create, update and delete transaction data based on said dispute and a predetermined security level to facilitate disposition of said transaction within said access controlled environment;

at an authentication facility, requiring said user to enter authentication data related to said transaction data in order to authenticate said transaction data based on a predetermined authentication scheme;

at said transaction management facility, permitting said user to enter said authentication data;

at said transaction management facility, notifying said user if a decision needs to be made based on said transaction data and/or said authentication data;

at said transaction management facility, allowing said user to enter a decision in order to dispose of said dispute;

at a communications facility, notifying said plurality of transaction parties of said decision via said global data network;

at a billing facility, consolidating data related to internal operations performed by said access control facility, said transaction management facility, and said authentication facility; and

at said billing facility, generating and processing said billing data and sending a billing notice to at least one of said transaction parties via said global data processing network.

117. The method according to claim 116, wherein said global data processing network is the Internet.

118. The method according to claim 116, wherein said access control facility includes a user registration facility permitting a user to be registered based on predetermined registration

criteria prior to permitting said user to access said access controlled environment.

119. The method according to claim 116, wherein said access control facility permits or denies access to said access controlled environment based on a user identifier and a user password.

120. The method according to claim 116, further comprising the step of: at said access control facility, notifying said responsible party when a user is denied access to said access controlled environment.

121. The method according to claim 116, wherein said transaction management facility is configured to store and maintain said data in ways corresponding to the type of said transaction.

122. The method according to claim 116, further comprising the step of: at said transaction management facility, generating internal tracking data corresponding to access and use of said transaction data by said user within said access controlled environment.

123. The method according to claim 116, wherein said transaction management facility stores said transaction data in a plurality of formats corresponding to associated systems maintained by external systems.

124. The method according to claim 116, wherein said predetermined security level corresponding to a predetermined data encryption scheme.

125. The method according to claim 116, further comprising the step of setting said predetermined security level by said user.

126. The method according to claim 116, further comprising the step of: at said transaction management facility, setting said predetermined security level automatically based on the type of said transaction.

127. The method according to claim 116, wherein said authentication scheme corresponds to rules of evidence.

128. The method according to claim 116, wherein said authentication scheme corresponds to rules of verification.

129. The method according to claim 116, wherein said authentication scheme is automatically set by said authentication system based on the type of said transaction.

130. The method according to claim 116, wherein said authentication facility further authenticates said transaction data based on the identity of said user.

131. The method according to claim 116, wherein said authentication facility authenticates said transaction data prior to said transaction management facility storing and maintaining said transaction data.

132. The method according to claim 116, wherein said authentication facility authenticates said transaction data after said transaction management facility stores and maintains said data.

133. The method according to claim 116, further comprises the step of: at said billing facility, generating a billing record related to each operation performed by said user within said access controlled environment.

134. The method according to claim 116, further comprising the step of: at said transaction management facility, automatically notifying said user when a change has occurred to said transaction data.

135. The method according to claim 134, wherein said transaction management facility notifies said user via an automatically generated electronic mail message.

136. The method according to claim 135, wherein said automatically generated electronic mail message contains a reference to said transaction based on a predetermined level of vagueness.